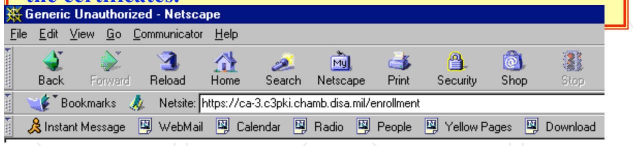
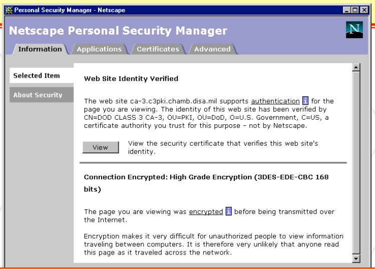
13 Your PKI Identity Certificate has been stored in the web browser. From the toolbar, click the Security icon. Make sure you have a floppy diskette to backup the certificates.


Generic Unauthorized - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks
Instant Message WebMail Calendar Radio People Yellow Pages Download

Netsite: https://ca-3.c3pki.chamb.disa.mil/enrollment

14 A *Netscape Personal Security Manager* window will appear. Click on the Certificates tab.



Web Site Identity Verified

The web site ca-3.c3pki.chamb.disa.mil supports authentication for the page you are viewing. The identity of this web site has been verified by CN=DOD CLASS 3 CA-3, OU=PKI, OU=DoD, O=U.S. Government, C=US, a certificate authority you trust for this purpose - not by Netscape.

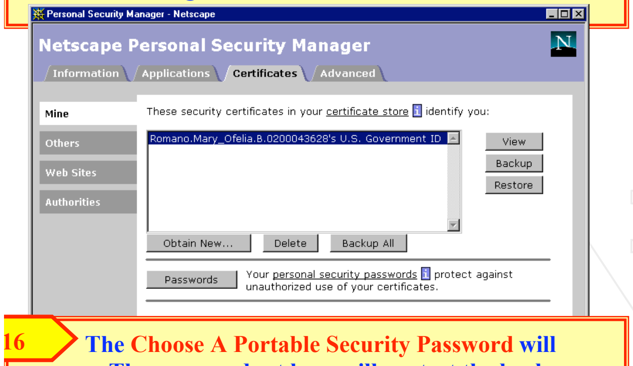
View the security certificate that verifies this web site's identity.

Connection Encrypted: High Grade Encryption (3DES-EDE-CBC 168 bits)

The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it very difficult for unauthorized people to view information traveling between computers. It is therefore very unlikely that anyone read this page as it traveled across the network.

15 Click to highlight the certificate you just downloaded. The certificate name will be the one with your Last Name appearing first; First name, second; followed by the 10-digit User Number you entered during the registration process. If you do not see the desired certificate, STOP and notify your Local Registration Authority (LRA) of the situation. Otherwise, highlight your entry and click the Backup button on the right-hand side of the screen to continue.

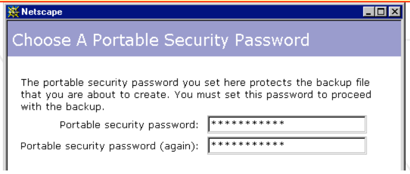


These security certificates in your certificate store identify you:

Romano.Mary_Ofelia.B.0200043628's U.S. Government ID

Your personal security passwords protect against unauthorized use of your certificates.

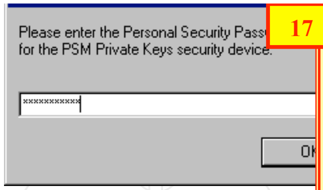
16 The Choose A Portable Security Password will appear. The password set here will protect the backup file that you are creating. Click the OK button. If you forget this password, you will not be able to restore this



The portable security password you set here protects the backup file that you are about to create. You must set this password to proceed with the backup.

Portable security password: ***********

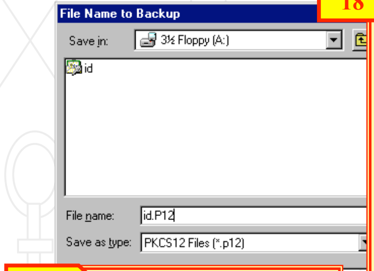
Portable security password (again): ***********



Please enter the Personal Security Pass for the PSM Private Keys security device.

****

17 The *Password Entry Dialog* box will appear. Enter your personal security password (created in step 10). Click the OK button.



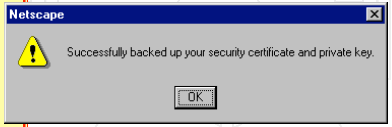
Save in: 3½ Floppy (A:)

File name: id.P12

Save as type: PKCS12 Files (*.p12)

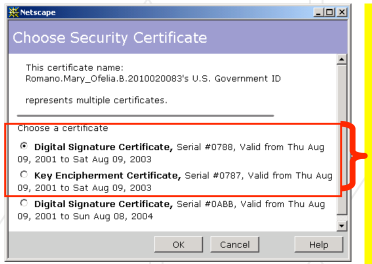
18 The *File Name to Backup* dialog box will appear. Insert a blank formatted floppy disk into the workstation's floppy disk drive. Select the floppy drive (A:) in the *File Name* location box. Type id.P12 in the file name field, then click the Save button.

19 The *successfully backed up your security certificate and private key* message will appear. Click the OK button to continue. Exit the *Netscape Personal Security Manager* window by clicking the Close button.



Successfully backed up your security certificate and private key.

20 You will have the repeat the process to obtain your digital signature and encryption certificates. Begin by getting your signature certificates and repeat process for your Key Encipherment Certificate. Enter Email.P12 for the signature certificate and encryptID.P12 for the encryption certificate.



This certificate name:
Romano.Mary_Ofelia.B.2010020083's U.S. Government ID

represents multiple certificates.

Choose a certificate

● **Digital Signature Certificate,** Serial #0788, Valid from Thu Aug 09, 2001 to Sat Aug 09, 2003

○ **Key Encipherment Certificate,** Serial #0787, Valid from Thu Aug 09, 2001 to Sat Aug 09, 2003

○ **Digital Signature Certificate,** Serial #0ABB, Valid from Thu Aug 09, 2001 to Sun Aug 08, 2004

This is your Email Signature and Encryption Certificates. The email and encipherment certificates should have the same expiration date. Their validity dates run for 2 years, while the ID certificates are valid for 3 years.

SPAWAR PKI

Department of the Navy
PKI Helpdesk
1.800.304.4636
itac@infosec.navy.mil

Quick Reference Guide for Downloading DoD PKI Class 3 Certificates

PUBLIC KEY INFRASTRUCTU

SPAWAR

After visiting your Local Registration Authority (LRA), you will be given a one page DoD PKI Certificate Registration Instruction (CRI) sheet. Th
CRI sheet contains the web site to download DoD PI
certificates. The CRI should be safeguarded, until y
have completed the certificates downloading process

NOTE: You will need to be using Netscape Communicator 4.7 or higher with Personal Security Manager (PSM) loaded onto your workstation. You can obtain a copy of both Netscape Communica
and PSM from http://netscape.intdec.com/disa.

You will need to install Netscape Communicator first.

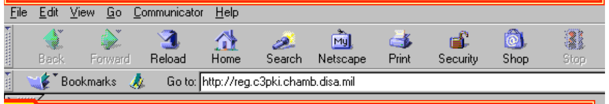
To install Netscape Personal Security Manager on Windows 95/98/2000/NT for use with Communicator 4.7 or later, save the fil
a convenient location with the specified filename, then drag the file
icon into a Navigator window (that is, a browser window displayed
Communicator). Dropping the file's icon over the browser window
initiates SmartUpdate, which automatically installs Personal Secur
Manager. After installation is complete, exit Communicator and
relaunch it. If your copy of Communicator is installed in the default
location, SmartUpdate installs the Personal Security Manager files
the directory
C:\ProgramFiles\CommonFiles\NetscapeShared\Security\ and add
the file cmnav.dllin the directory C:\Program Files\Netscape\Communicator\Program.

To install Personal Security Manager for use with Communicator 4
or later on Unix, you must be logged in as the same Unix user you
be logged in as when you run Communicator. For the Unix installa
to succeed, you must have write privileges for both the directory
where the Netscape executable resides and the directory where th
installation script creates the directory containing the Personal
Security Manager files. To install Personal Security Manager for us
with Communicator 4.7x, download the tar file for the version of the
product that you want to install and follow these steps:

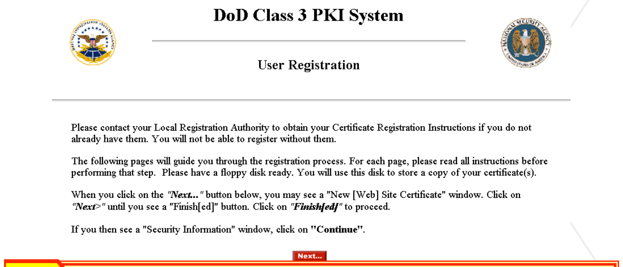
1. Exit Communicator, if it is running.
2. Decompress the downloaded file to some convenient location.
3. Run the psm-install program.

The psm-install program allows you to specify the directory in whic
Personal Security Manager will be installed. In this release, you mu
install Personal Security Manager locally. To do so, you can either
install it in the default location (/opt/netscape/security) or in some
other local location. However, if you install Personal Security Mana
anywhere other than the default location, Communicator must also
installed locally. To run Personal Security Manager on Unix, you m
be logged in as the same Unix user you were logged in as when y
installed it.

1 Open *Netscape Communicator* (4.7 or higher) and type the web site address found on the Certificate Registration Instruction sheet. Press the Enter key.


File Edit View Go Communicator Help
Back
Forward
Reload
Home
Search
Netscape
Print
Security
Shop
Stop
Bookmarks
Go to: http://reg.c3pki.chamb.disa.mil

2 Read the information related to the registration process located on the *User Registration* page. Click the Next button to continue.



DoD Class 3 PKI System

User Registration

Please contact your Local Registration Authority to obtain your Certificate Registration Instructions if you do not already have them. You will not be able to register without them.

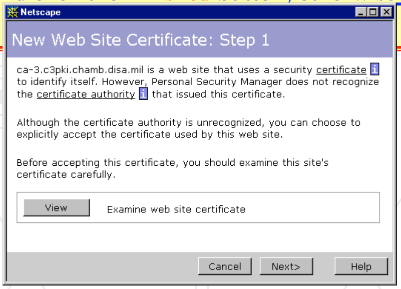
The following pages will guide you through the registration process. For each page, please read all instructions before performing that step. Please have a floppy disk ready. You will use this disk to store a copy of your certificate(s).

When you click on the *"Next..."* button below, you may see a "New [Web] Site Certificate" window. Click on *"Next>"* until you see a "Finish[ed]" button. Click on ***"Finish[ed]"*** to proceed.

If you then see a "Security Information" window, click on **"Continue"**.

Next...

3 The *New Web Site Certificate Step 1* window appears, click the Next button. Accept the default selection on the *New Web Site Certificate Step 2* window and click the Finished button; otherwise go to Step 4.



Netscape

New Web Site Certificate: Step 1

ca-3.c3pki.chamb.disa.mil is a web site that uses a security certificate to identify itself. However, Personal Security Manager does not recognize the certificate authority that issued this certificate.

Although the certificate authority is unrecognized, you can choose to explicitly accept the certificate used by this web site.

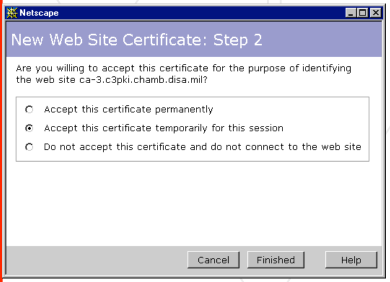
Before accepting this certificate, you should examine this site's certificate carefully.

View Examine web site certificate

Cancel Next> Help

4 Read the text and follow the on-screen directions to download the Class 3 Root CA Certificate and the Medium Assurance Root CA Certificate into the Netscape browser Certificate database.

NOTE: If you receive a message that states: "Certificate cannot be imported. This certificate is already in your database," click OK to continue. Be sure that both root certificate authorities have been downloaded into the Netscape browser.



Netscape

New Web Site Certificate: Step 2

Are you willing to accept this certificate for the purpose of identifying the web site ca-3.c3pki.chamb.disa.mil?

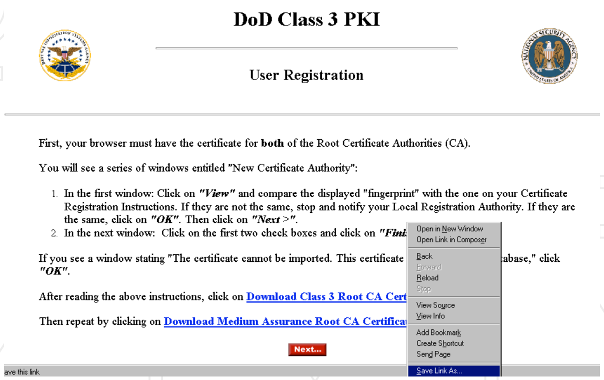
○ Accept this certificate permanently
● Accept this certificate temporarily for this session
○ Do not accept this certificate and do not connect to the web site

Cancel Finished Help

5 Right click on the Download Class 3 Root CA Certificate. Select the *Save Link As* option.

6 The *Save As. . .* window will appear. Insert a blank formatted floppy disk into the workstation's floppy disk drive. Select the floppy drive (A:) in the *Save in* location box. Type DODROOT.P7B in th File Name field and then click the Save button.

7 Repeat steps 5 and 6 to save the Medium Assurance Root CA Certificate to the floppy disk. Name the Medium Assurance Root MEDROOT.P7B.



DoD Class 3 PKI

User Registration

First, your browser must have the certificate for **both** of the Root Certificate Authorities (CA).

You will see a series of windows entitled "New Certificate Authority":

1. In the first window: Click on ***"View"*** and compare the displayed "fingerprint" with the one on your Certificate Registration Instructions. If they are not the same, stop and notify your Local Registration Authority. If they are the same, click on ***"OK"***. Then click on ***"Next >"***.
2. In the next window: Click on the first two check boxes and click on ***"Fini***

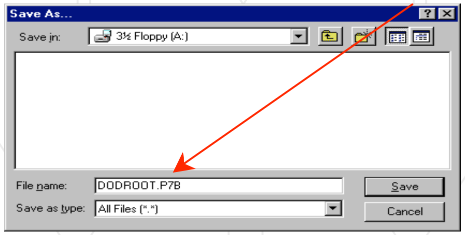
If you see a window stating "The certificate cannot be imported. This certificate abase," click ***"OK"***.

After reading the above instructions, click on Download Class 3 Root CA Cert

Then repeat by clicking on Download Medium Assurance Root CA Certifica

Next...

ave this link



Save As...

Save in: 3½ Floppy (A:)

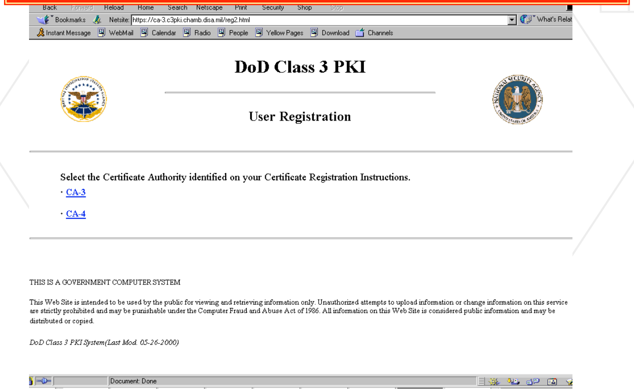
File name: DODROOT.P7B

Save as type: All Files (*.*)

Save

Cancel

8 You will be returned to the *User Registration* window. Click the Next button to continue. Select the designated CA server as indicated on the Certificate Registration Instruction (CRI) sheet.


Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks
Netsite: https://ca-3.c3pki.chamb.disa.mil/reg2.html
What's Related
Instant Message WebMail Calendar Radio People Yellow Pages Download Channels

DoD Class 3 PKI

User Registration

Select the Certificate Authority identified on your Certificate Registration Instructions.

- CA-3
- CA-4

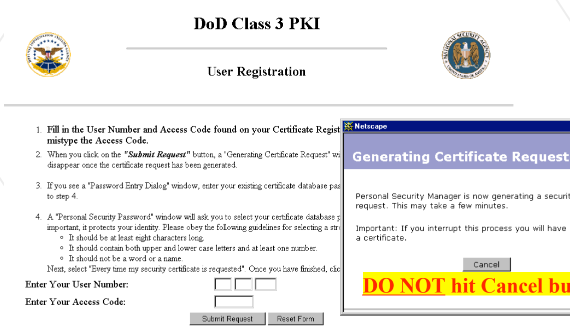
THIS IS A GOVERNMENT COMPUTER SYSTEM

This Web Site is intended to be used by the public for viewing and retrieving information only. Unauthorized attempts to upload information or change information on this service are strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1986. All information on this Web Site is considered public information and may be distributed or copied.

DoD Class 3 PKI System(Last Mod. 05-26-2000)

Document: Done

9 Enter the *User Number* and *Access Code* from the C sheet. Be careful not to mistype the Access Code. Click Submit Request button. The *Generating Certificate Re* window will appear.



DoD Class 3 PKI

User Registration

1. **Fill in the User Number and Access Code found on your Certificate Regist mistype the Access Code.**
2. When you click on the ***"Submit Request"*** button, a "Generating Certificate Request" wi disappear once the certificate request has been generated.
3. If you see a "Password Entry Dialog" window, enter your existing certificate database pas to step 4.
4. A "Personal Security Password" window will ask you to select your certificate database p important, it protects your identity. Please obey the following guidelines for selecting a str
   - It should be at least eight characters long.
   - It should contain both upper and lower case letters and at least one number.
   - It should not be a word or a name.

   Next, select "Every time my security certificate is requested". Once you have finished, clic

Enter Your User Number: □ □ □

Enter Your Access Code: □

Submit Request Reset Form

Netscape

Generating Certificate Request

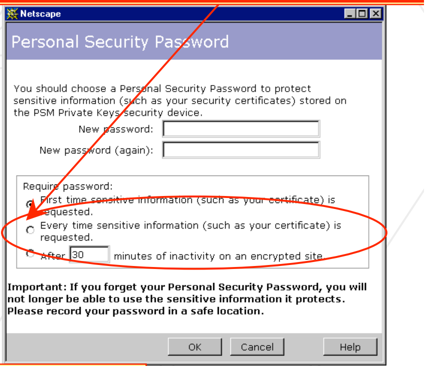
Personal Security Manager is now generating a securit request. This may take a few minutes.

Important: If you interrupt this process you will have a certificate.

Cancel

DO NOT hit Cancel bu

10 The *Personal Security Password* window will app Create a password for the PSM Private Key device; otherwise enter the password for the PSM Private Key Select the "Every time sensitive information (such as y certificate) is requested." option. Click the OK button continue. Proceed to step 11.



Netscape

Personal Security Password

You should choose a Personal Security Password to protect sensitive information (such as your security certificates) stored on the PSM Private Keys security device.

New password:

New password (again):

Require password:

● First time sensitive information (such as your certificate) is requested.

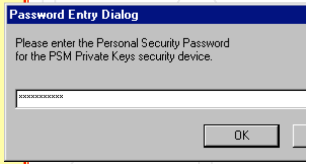
○ Every time sensitive information (such as your certificate) is requested.

○ After 30 minutes of inactivity on an encrypted site.

Important: If you forget your Personal Security Password, you will not longer be able to use the sensitive information it protects. Please record your password in a safe location.

OK Cancel Help

11 The *Personal Entry Dialog* box may appear. Enter your personal security password. Then click OK button. This is the password created in step 10.

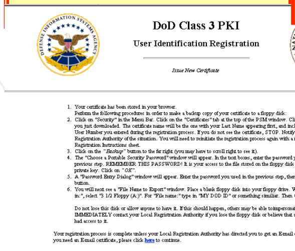


Password Entry Dialog

Please enter the Personal Security Password for the PSM Private Keys security device.

****

OK



DoD Class 3 PKI

User Identification Registration

Issue New Certificate

1. Your certificate has been stored in your browser. Perform the following procedures in order to make a backup copy of your certificate to a floppy disk:
2. Click on "Security" in the Menu Bar. Click on the "Certificates" tab at the top of the PSM window. Click on the certificate you just downloaded. The certificate name will be the one with your Last Name appearing first, and includes the 10 digit User Number you entered during the registration process. If you do not see the certificate, STOP. Notify your Local Registration Authority of the situation. You will need to reinitiate the registration process again with a new Certificate Registration Instructions sheet.
3. Click on the *"Backup"* button to the far right (you may have to scroll right to see it).
4. The "Choose a Portable Security Password" window will appear. In the text boxes, enter the password you created in the previous step. REMEMBER THIS PASSWORD! It is your access to the file stored on the floppy disk containing your private key. Click on *"OK"*.
5. A "Password Entry Dialog" window will appear. Enter the password you used in the previous step, then click the *"OK"* button.
6. You will next see a "File Name to Export" window. Place a blank floppy disk into your floppy drive. Where you see "Save in:", select "3 1/2 Floppy (A:)". For "File name:" type in "MY DOD ID" or something similiar. Then Click on *"Save"*.

   Do not lose this disk or allow anyone to have it. If this should happen, others may be able toimpersonate you electronically. IMMEDIATELY contact your Local Registration Authority if you lose the floppy disk or believe that someone else has had access to it.

Your registration process is complete unless your Local Registration Authority has directed you to get an E-mail certificate also. If you need an E-mail certificate, please click here to continue.

12 Read and follow o screen instructions, located on the *User Registration* page, to download your Ident Certificate into the Netscape Communicator browser.